
دار المنظومة
DAR ALMANDUMAH

الجريمة الالكترونية بين تحديات الواقع واستشراف المستقبل

د. خالد علي الجنيبي*
رئيس نيابة عامة
نيابة دبي
الامارات العربية المتحدة

الملخص— لا مناص من ان غاية تسليط الضوء على الجرائم الالكترونية لا يرجع الي خطورتها فحسب، وإنما أيضاً إلي العديد من التطورات التي استلزمت طرح موضوع الدراسة واستظهار كافة الجوانب المؤثرة في الحد من استفحال خطر الجريمة الالكترونية على المستويين المحلي والدولي. ففي اطار سعي الدول نحو تعزيز الوعي بخطورة الجرائم الالكترونية، وما ينتج عنها من تهديد للأمن المعلوماتي والاقتصادي والثقافي والاجتماعي، ورغبة بعض الدول في تهيئة مناخ من الثقة لإقامة الحكومات الذكية والتي باتت مطلباً ضرورياً لكثير من الدول والشعوب. اضحت الجرائم الالكترونية تحظى بأهمية لا يجادل فيها احد سواء على المستوى الفردي او القانوني او حتى الاعلامي ومع استفحال خطرها وملامستها لجوانب شتى في المجتمع برزت اهمية دراسة حالتها ، هذه الاهمية كانت المولد الاول لطرح هذا الموضوع. فالجرائم الإلكترونية تكتسي اهمية خاصة تنبع ليس من خطورتها فقط ، وانما أيضاً لأثارها العديدة سواء على الصعيد الاجتماعي او الاقتصادي او القانوني او حتى السياسي. فكان لا بد من تسليط الضوء على أهمية التعليم والتدريب في مجال الجرائم الالكترونية وادلة إثباتها حيث ان الوصول الى غاية الحد من الجرائم الالكترونية ينبغي ان ينطلق من حقيقة هامة الا وهي " ان فهم الجريمة اهم من نصوص تجريمها". فجاءت هذه الورقة المعنون لها بـ « الجريمة الالكترونية بين تحديات الواقع واستشراف المستقبل »، متبعين في ذلك المنهج الوصفي. وقد خلص البحث الى ان الجريمة الالكترونية اصبحت واقع حال وليست سحابة صيف ، هذا الواقع يحتم علينا تلميم اوراقنا واعداد عدتنا لمواجهة هذا الخطر المستفحل الذي اصاب مجتمعنا اجتماعياً واقتصادياً وقانونياً. إن النصوص التشريعية المحدثة او المستحدثة تحتاج الى سواعد وعقول مبصرة مدركة قادرة على تطبيقها بالشكل السليم والصحيح . فالمستوى المعرفي بالجريمة الالكترونية يجب أن يرتقي ويتطور بتطور الجريمة ونصوص تشريعها، هذا الوعي يجب أن يرسم له مسار ينطلق من المراحل الاولى من التعليم الجامعي لينمو على اساس سليم ويتطور بتطور الادراك المعرفي اللاحق للحياة الجامعية.

١. مقدمة

شاع مصطلح الجريمة الالكترونية في الآونة الاخيرة مع شيوع استخدام التكنلوجيا ، فتعددت صيغ اصطلاحها تعدداً حمل ثراء التنوع والاتساع لا الضيق والتضاد.

فمع اختراع الحاسب الآلي والذي أعد أحد أهم الاختراعات البشرية في أوخر القرن الماضي وما صاحبة من إنجازات بشرية في مجالات شتي برزت اوجه اخرى لاستخدام التكنلوجيا فإنحرف مسارها الصحيح واستغلت في تبسيط وتيسير ارتكاب الجرائم ، فكان للمجرمين ما سعو الية فأضحت التكنلوجيا وسيلة جريمة وانتهاك لا وسيلة رقي وتقدم. ومع ثراء التكنلوجيا وسرعة تطورها تفنن المجرمين في أساليب ارتكابها حتى غدت طلاسم ورموز احتاج حل رموزها مفكرين لا مجرد منفذين للقانون. وفي الجانب الاخر اختلفت ادلة اثبات الجرائم الالكترونية باختلاف خصائصها فكان لازماً منا فهم الجريمة الالكترونية فهماً أعمق، ودراسة حالتها دراسة متأنية شمولية بوصفها واقعاً أثر في حياتنا واقتصادنا ونظمنا القانونية والقضائية.

لا مناص من أن معظم الدول سعت الي تحديث نصوص قوانينها او حتى إصدار تشريعات خاصة جرمت من خلالها أنماط السلوك الغير مشروع الممارس عن طريق إستخدام التكنلوجيا فأهتمت بذلك بجانب هام الا وهو جانب التشريع، الا انها قد تكون قد اغفلت عن جانب آخر لا يقل أهمية الا وهو جانب الوعي والتثقيف.

هذه الورقة سوف تسعى الى إبراز أهمية التعليم والتدريب في مجال الجرائم الالكترونية وادلة إثباتها حيث

* باحث متخصص في مجال الجريمة الالكترونية وادلة اثباتها ، له منشورات علمية منها على سبيل المثال لا الحصر:
- 'Search and seizure for electronic evidence: procedural aspects of UAE's legal system', Digital Evidence and Electronic Signature Law Review UK 10 (2013).
- 'The Legal Regulation of E-Commerce and Cloud

ان الوصول الى غاية الحد من الجرائم الالكترونية ينبغي ان ينطلق من حقيقة هامة الا وهي " ان فهم الجريمة اهم من نصوص تجريمها". فجاءت هذه الورقة المعنون لها بـ: « الجريمة الالكترونية بين تحديات الواقع واستشراف المستقبل »، ضمن فعاليات المؤتمر الدولي الاول للجرائم المعلوماتية خلال الفترة ١٠ـ١٢/١١/٢٠١٥م بالمملكة العربية السعودية

٢. المبحث الاول: مقدمات تعريفية

المطلب الاول: تعريف الجريمة الالكترونية:

من اهم التعريفات التي قيلت في تعريف الجريمة الالكترونية تعريف منظمة التعاون الاقتصادي والتنمية (OCDE)؛ إذْ عَرَّفت الجريمة الالكترونية في اجتماع باريس عام (١٩٨٣م) بأنها: (كل سلوك غير مشروع أو غير أخلاقي أو غير مصرَّح به، يتعلّق بالمعالجة الآليّة للبيانات أو نقلها).[1]

وفي الإطار العربي جاء تعريف الجريمة الإلكترونية حينما أقامت الجامعة العربية الندوة العربية في ١٩٩٨/٢/١م في إطار تعريف الجريمة المنظمة حيث عرفت الجريمة المنظمة بأنها :(كل سلوك إجرامي ترتكبه مجموعة من الأشخاص يحترفون الإجرام بشكل مستمر لتحقيق أهدافهم ضمن نطاق أكثر من دولة)، فدار رحى تعريف الجريمة الالكترونية في فلك تعريف الجريمة المنظمة.

اما في الجانب التشريعي فنجد أن البعض عمد الي تعريف الجريمة الالكترونية في نصوص تشريعية كما هو الحال في التشريع السعودي حيث عَرّف نظام مكافحة جرائم المعلوماتية السعودي، الصادر بالمرسوم الملكي رقم م/ ١٧ المؤرخ في: ١٤٢٨/٣/٨هـ بناءً على قرار مجلس الوزراء رقم: (٧٩) المؤرخ في: ١٤٢٨/٣/٧هـ الجريمة الالكترونية بأنها:(أي فعل يُرتكب متضمّنًا استخدام الحاسب الآلي أو الشبكة المعلوماتية بالمخالفة لأحكام هذا النظام).[2] كما هو الحال ايضاً حينما عرف قانون رقم (١٤) لسنة ٢٠١٤م في شأن مكافحة الجرائم الالكترونية القطري الجريمة الإلكترونية بانها: (أي فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية، بطريقة غير مشروعة، بما يخالف أحكام القانون).[3]

بينما نحى البعض الاخر الي مجرد الإشارة الى انماط الجريمة الالكترونية دون تعريفها كما فعل التشريع الاماراتي حين بين مرسوم بقانون اتحادي رقم (٥) لسنة ٢٠١٢ م في شأن مكافحة جرائم تقنية المعلومات (كما جاء في صياغة نصوصه) الجريمة الالكترونية بأنها: (كل أشكال السلوك غير المشروع الذي يُرتكب باستخدام الشبكة المعلوماتية أو وسيلة تقنية معلومات).[4]

المطلب الثاني: تبعة الارتباط بين الانترنت والحاسب الالي

أدي ارتباط شبكة الانترنت بالحاسب الألي ارتباطاً وثيقاً الى وجود ارتباط بين الجريمة المتعلقة بالحاسب الالي CrimeComputer( ) والجريمة المتعلقة بشبكة الانترنت Crime(Internet) ، مع وجود فارق زمني فيما بين بداية ظهور كل منهما، حيث أرجع الفقه الجنائي جرائم الحاسوب الى عام ١٩٥٨م، في حين بدأت جرائم شبكة الإنترنت مع بداية إطلاق شبكة الإنترنت عام ١٩٨٨.[5]

ولن نخوض في الخلاف الفقهي حول التعريفات التي وضعت لجرائم الحاسب الالي او لجرائم شبكة الإنترنت مكتفين بما سبق بيانة بشأن تعريف الجريمة الالكترونية بصورة شمولية منوهين فقط بتعدد الاصطلاحات التي وضعت تعريفاً لجرائم الحاسب الالي والتي عرفت شمولاً بأنها الجرائم التي يكون الحاسوب الالي هدفاً لها او وسيلة لارتكابها او أداة لحفظ الادلة ، ولجرائم شبكة الانترنت والتي عرفت شمولاً ايضاً بأنها الجرائم التي ترتكب بواسطة الأداة التواصلية بين الشبكات دون اعتبار للحدود الجغرافية منوهين من وجود صعوبة في الفصل بين الجريمتين.

٣. المبحث الثاني: التأثير الاجتماعي والاقتصادي للجريمة الالكترونية

لا مناص من الاعتراف من اننا أصبحنا في عالم أزالت التقنية فيه حدود الاتصال، وسادت ثقافات العولمة

---

(1) انظر: www.oecd.org.

(2) انظر: المادة رقم (١) من نظام مكافحة جرائم المعلوماتية السعودي.

(3) انظر: المادة رقم (١) من القانون رقم (١٤) لسنة ٢٠١٤ م في شأن مكافحة الجرائم الالكترونية القطري.

(4) مرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ م في شأن مكافحة جرائم تقنية المعلومات جاء استبدالا للقانون رقم (٦) لسنة ٢٠٠٦ م.

(5) أنظر: د. محمد الشوا ، الغش المعلوماتي كظاهرة إجرامية مستحدثة ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة ، ٢٥/٢٨ أكتوبر ١٩٩٣، ص ٢.

الشعوب والاقطار. فمع انتشار التقنية ظهرت تيارات الحماس والقلق، الحماس من اجل استخدام التقنية في وسائل الاتصال فانعدمت المسافات بين الشعوب والافراد وعقدت الصفقات عن بعد وفتحت اسواق وآفاق دون عناء، اما القلق فمن اجل احتمال عدم تأمين الاستخدام السليم للوسائل التقنية استهدفت المعطيات بدلالتها التقنية الواسعة (بيانات، معلومات، وبرامج بكافّة أنواعها) بالاعتداء فقرعت الشعوب في جنباتها أجراس الخطر لتنبّه المجتمعات لحجم المخاطر وهول الخسائر وهواجسها. فالجريمة الالكترونية تنشأ في الخفاء، يقترفها مجرمون أذكياء، يمتلكون أدوات المعرفة التقنية، تُوَجَّه للنَّيْل مِنَ الحق في المعلومات، وتَطَال اعتداءاتها معطيات الحاسب الالي المخزَّنة، والمعلومات المنقولة ، عبر نُظُم وشبكات.

لن نخوض كثيراً في التقارير ونتائج الدراسات التي اجريت لبيان حجم الخسائر وعدد ضحايا الجرائم الالكترونية فما يهمنا هنا فعلاً أن نشير فقط الي أن حجم الخسائر الفعلية للجرائم الالكترونية قد فاق مبلغ (113bn) دولار أميركي وأن عدد ضحايا الجرائم الالكترونية بلغ (٣٧٨) مليون ضحية حول العالم بمعدل (١٢) ضحية كل ثانية في عام ٢٠١٣م.[1]

هذه الارقام وإن كانت تمثل إحصائيات الا انها قد تكون اقل بكثير من الارقام الحقيقية ، فغالباً لا تفضل الشركات والمؤسسات الابلاغ عن تعرضها لجرائم او مخاطر خوفاً على السمعة والمراكز المالية وعلى الجانب الفردي قلة من الضحايا على وعي ومعرفة بطرق الابلاغ عن الجرائم او ربما انهم قد لا يعلمون اصلا انهم وقعوا ضحايا لجرائم ذوي الياقات البيضاء.

وأمّا عن الخطورة الأخلاقية والاجتماعية؛ فإنَّ جلّ الجرائم الالكترونية تستهدف فضح الأسرار الشخصيّة أو القذف أو التشهير اما بأشخاص أو بشركات إضراراً بالسمعة الشخصية أو المالية، إمّا بداعي المنافسة، أو بسبب الانتقام ، ونحو ذلك. فعبر ملايين المواقع تُنشَر الصور المخلة بالحياء، وتُقدِّم الخدمات الجنسيّة ، وتُستغل الصور والمقاطع البصرية للأشخاص عموماً والاطفال خصوصاً في أوضاع شائنة ، دون أن تبسط على تلك الأنشطة يد القوانين المحليّة أو الدولية.[2]

إن ما يهمنا ابرازه هنا هو أن التحولات الاجتماعية والاقتصادية والتي كانت وليدة الطفرة في المجال التقني صاحبها سعي معرفي وقانوني للتصدي ولمل الفراغ التشريعي الناتج عن النقيض السلبي لتلك الطفرة التقنية وذلك سعياً من اجل ايجاد الحلول التشريعية لأنماط السلوك الغير مشروع المصاحب للاستخدام السلبي للتكنلوجيا ، وعلية فإن السؤال المطروح على بساط البحث: هل بلغت تلك المساعي مبتغاها ام لازالت في مراحل البحث عن الحلول الناجعة لإشكال الجرائم المستحدثة, وهل المستوى المعرفي ملائم لفهم اسبار الجرائم الالكترونية وطرق ارتكابها ام لازلنا بعيدين عن الادراك المعرفي ، هذا ما سوف نسعى للإجابة عنة في قادم نقاط البحث.

٤. المبحث الثالث: الجريمة الالكترونية في مواجهة الجريمة التقليدية

اذ ما طرح سؤال: هل يمكنك التفريق بين الجريمة في مفهومها التقليدي والجريمة الالكترونية؟ فأن الاجابة قد تكون وللوهلة الاولى بسيطة يسيرة : (نعم) يوجد فرق ولكن مع تعمق الاجابة نجد أن الامر يحتاج الى شروحات وتفاسير قد يصعب على المتلقي ذو الثقافة القانونية البسيطة فهمها. فالجريمة الالكترونية واذ ما كانت تشترك مع الجريمة التقليدية في اركانها المتعارف عليها قانوناً من ركن مادي ومعنوي وعلاقة سببية بين الفعل والنتيجة ، الا انها تختلف باختلاف طرق ارتكابها وادلتها والتي يعصب على رجال القانون فهمها. فالجريمة الالكترونية ذات مسرح افتراضي لا حدود جغرافية له تتعامل مع رموز ومعطيات الالكترونية غير مادية وغير ملموسة ، فالاختلاف مثلاً بين الدليل في الجريمة التقليدية والدليل في الجريمة الالكترونية هو الدعامة التي يكون عليها كل منهما ، فالأدلة التقليدية دعامتها اشياء مادية ملموسة، بعكس الادلة الالكترونية ، فان دعامتها رموز واشارات، واعتمادا علي هذا الفارق في التكوين، والوجود، يري البعض أن الدليل الإلكتروني، لا يكتسب صفة الدوام والاستقرار والثبات ، اذ انه قابل للمحو والتعديل والاتلاف ،

---

(1) انظر: تقرير "TheNorton Cybercrime Report 2013"، http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

(2) د. فايز بن عبدالله الشهري، التحديات الأمنية لوسائل الاتصال الجديدة – دراسة الظاهرة الإجرامية على شبكة الإنترنت، – دراسة الظاهرة الإجرامية على شبكة الإنترنت، المجلة العربية للدراسات الأمنية والتدريب، المجلد ٢٠، العدد ٣٩، (ص١٥٤ – وما بعدها).

كما انه غير قابل للقراءة او المشاهدة البصرية وانما هو نتاج تحاليل مختبرات لها شروطها الخاصة.

إن كانت القاعدة في الدعاوى الجنائية هي جواز الإثبات بكافة طرق الاثبات القانونية ، والقيد على هذه القاعدة ان الدليل يتعين أن يكون من الادلة التي يقبلها القانون ، وبالتالي قد يعترف بالدليل ذو الطبيعة الالكترونية ، الا أن هذا الاعتراف قد يكون مشروطاً بقناعة القاضي واطمئنانه للدليل ولن نصل الي هذا الاقتناع من غير فهم كامل وكاف لطبيعة وخصائص الجريمة الالكترونية وادلة اثباتها.

من هنا ظهرت الحاجة الى وجود فهم أعمق للجريمة الالكترونية المستحدثة وادلة اثباتها، فوفق دراسة غير منشورة قام بها الباحث على شريحة من القضاة واعضاء النيابة العامة والمحامين ورجال الشرطة خلال الفترة بين عامي ٢٠١٣ و ٢٠١٤ م بدولة الامارات العربية المتحدة ، وجد الباحث أن مستوى الوعى والمعرفة بالجريمة الالكترونية وادلة اثباتها متدنى وأن المعرفة قد لا تعدو الا معرفة النصوص القانونية المنظمة لأنماط السلوك غير المشروع الممارس والمنظم بالحماية الجنائية بموجب قانون مكافحة جرائم تقنية المعلومات.[1]

اهمية التعليم والتطوير لم يكونا بعيدين عن الدول الاجنبية، فقد تنبهت الية معظم الدول الاوروبية ولهذا عمدت الى رفع مستوى الوعي والمعرفة بالجرائم الالكترونية من خلال الدورات التدريبية والورش الفنية. فخلال الفترة بين عامي ٢٠٠٨ و٢٠١٠م عقدت دورة نظامية للدول الاعضاء بالاتحاد الاوربي وبريطانيا منحت الي اثرها شهادة معتمدة للقضاة واعضاء النيابة العامة في مجال الجرائم الالكترونية وادلة اثباتها وذلك من اجل رفع المستوى المعرفي والادراكي .[2]

كما كانت هناك دراسة متعمقة لواقع الحال بالاتحاد الاوروبي عام ٢٠٠٥م شملت (١٦) دولة من الاتحاد الاوروبي شارك فيها قضاة واعضاء نيابة ومحامين وأكاديميين متخصصين في مجال الجرائم الالكترونية توصلت تلك الدراسة الى ضرورة اتخاذ سياسة موحدة لمواجهة الجرائم الالكترونية وتنظيم ادلة اثباتها ورفع المستوى المعرفي والادراكي لدي اعضاء السلك القضائي والقانوي.[3]

من هذا نصل الي حقيقة هامة أن الجوانب المعرفية والادراكية مهمة في مسعي الحد من استفحال خطر الجريمة الالكترونية، وإن فهم الجريمة الالكترونية هو حجر الزاوية الذي ينبغي الانطلاق من خلاله في محاربة الجريمة الإلكترونية. ولن يتأتى ذلك من غير وجود نظام قانوني شمولي يعنى بمحاربة الجريمة الالكترونية يكون قوامة التكامل التشريعي بشقية العقابي والاجرائي ومن مستوى معرفي إدراكي بالجريمة الالكترونية وادلة اثباتها.

٥. المبحث الرابع: النموذج المقترح

ينطلق الاقتراح من نقطة هامة الا وهي أن سعي الدول نحو رفع المستوى المعرفي بالجريمة الإلكترونية من خلال عقد ورش العمل والندوات قد تغدو قاصرة عن بلوغ غاية عقدها خاصة مع استفحال الجريمة الإلكترونية ومسها شريحة كبيرة من فئات المجتمع. فالفئة المستهدفة من التطوير بسيطة وإمكانية التطوير والتعلم المستقبلي لتك الفئة محدود فضلاً عن أن هناك فئات وشرائح كثيرة تتعامل بشكل او بأخر مع الجريمة الإلكترونية قد لا تنال فرصة الانضمام لتك الدورات او ورش العمل فكانت هناك فجوة معرفية اثرت في التصدي للجريمة الإلكترونية وازدياد رقعة انتشارها. فرجال الضبط القضائي غير ملمين الالمام الكافي بطرق جمع الادلة الالكترونية والمحافظة عليها خاصة في ظل عدم وجود قواعد ارشادية او نصوص قانونية منظمة لطرق جمع الادلة الالكترونية. وعلىالجانب الاخر تقف المختبرات الجنائية عاجزة عند تحليل اوجمع ادلة الجريمة الالكترونية خاصة اذ ما تعلق الامر بتعارض الافصاح للمعلومة وحماية الحقوق الشخصية كحالة طلب معلومات عن مستخدم البريد الالكتروني المستخدم في الجريمة الالكترونية وحق الشركة في عدم الافصاح بدعوى حماية الحق في الخصوصية ، فضلاً عن ارتفاع كلفة التطوير والتدريب وغلاء ثمن اجهزة الفحص والتحليل . وفي مراحل التحقيق نجد صعوبة في فهم اركان الجريمة الالكترونية واصباغ الوصف القانوني الصحيح عليها اذ ما افترضنا جدلاً اكتمال التحقيق دون منقصات وجود بعض الادلة في دول اخري وما قد يعترض الحصول عليها من عدم وجود تعاون دولي في هذا شأن. اما مرحلة المحاكمة

---

(1) هذه الدراسة شملت شريحة بلغت (٢٠٠) متخصص قانوني موزعين على امارات الدولة السبع، استخدم فيها الباحث المنهج العلمي في جمع وتحليل البيانات.

(2) اطلق على البرنامج مسمي (Cybex) شمل (٢١) دولة اوروبية و(٣) دول من امريكا الجنوبية.

(3) تعد هذة الدراسة من اهم الدراسات الميدانية ، استخدم فيها المنهج العلمي في جمع وتحليل البيانات ، حيث تم مقابلة اكثر من (١٢٥) شخص متخصص في مجالة من قضاة واعضاء نيابة وضباط شرطة ومحامين واكاديمين.

فلا عجب اذ ما قلنا أن الجريمة الالكترونية من اصعب الجرائم على القضاة فهم اسبارها ، فالجريمة الالكترونية هي جريمة تقنية تغلفها التقنية في طرق ارتكابها ونتائجها واكتشافها. فالقاضي غير الملم بالأمور التكنلوجية والتقنية غير قادر على الوصول الي الاقتناع القضائي المنشود في الاحكام القضائية.

وعلية كان من الواجب على الجامعات والكليات الاكاديمية ان يكون لها الدور في المساهمة في خلق جيل واع بالجريمة الالكترونية من خلال اقرار مساقات دراسية يتم تضمينها البرامج الأكاديمية ، يدرس من خلالها الطالب الجريمة الالكترونية وادلة اثباتها بشكل نظامي فتتولد لدية المعرفة والدراية بالجرائم المستحدثة ، هذه المعرفة هي اللبنة الاولى التي من خلالها يمكن تطويرها وتنميتها بعد التخرج من واقع الحياة العملية والبرامج المتخصصة والتي يتم تصميمها بما يتناسب ومتطلبات كل مرحلة. فمع الاعتراف أن بعض الجامعات والكليات بدأت في تسليط الضوء على الجريمة الالكترونية الا انها قد لا تعدو محاولات لم يكتب لها الاكتمال المطلوب فلازالت الجريمة الالكترونية لم تحضي بالدراسة الاكاديمية شأنها شأن الجريمة التقليدية. فكان لازماً وفقاً لمعطيات العصر الحالي ومتطلباته أن تقر الجريمة الالكترونية كمساق يتم دراسته بشكل متعمق يقسم الى فرعي علم، قسم يتناول فيه دراسة الجريمة الالكترونية كشكل من اشكال الجرائم المستحدثة، وقسم آخر يعنى بدراسة ادلة اثبات الجريمة الالكترونية. فيتولد لدى طالب القانون الالمام الكاف بهذا النوع من الجرائم وهو ما قد يلبي متطلبات التطوير الذاتي المستقبلي.

ليس ذلك وحسب وانما يجب على الدول أن يكون لديها نظام إحصائي خاص بالجريمة الالكترونية يتم من خلاله رصد الجريمة وانماط سلوكها والفئات المستهدفة ، فمن خلال تلك المعطيات يمكن تصميم البرامج وتحديد الفئات المستهدفة من التطوير والتعلم.

٦. الخاتمة

ختاماً، قد لا تكون هذه الاوراق قد اوفت للموضوع حقة من ناحية العرض والتحليل فهناك دائما مبررات للاختصار. ما نود الوصول الية من خلال العرض السابق أن الجريمة الالكترونية اصبحت واقع حال وليست سحابة صيف ، هذا الواقع يحتم علينا تلميم اوراقنا واعداد عدتنا لمواجهة هذا الخطر المستفحل الذي اصاب مجتمعنا اجتماعياً واقتصادياً وقانونياً. إن النصوص التشريعية المحدثة او المستحدثة تحتاج الى سواعد وعقول مبصرة مدركة قادرة على تطبيقها بالشكل السليم والصحيح . فالمستوى المعرفي بالجريمة الالكترونية يجب أن يرتقي ويتطور بتطور الجريمة ونصوص تشريعها، هذا الوعي يجب أن يرسم له مسار ينطلق من المراحل الاولى من التعليم الجامعي لينمو على اساس سليم ويتطور بتطور الادراك المعرفي اللاحق للحياة الجامعية . فلن تجدي الدورات والندوات صنعاً في خلق جيل قادر على مجابهة الجريمة المستحدثة لوحدها بل يجب ان تبنى المعرفة من بداية تعلم القوانين بالمراحل الجامعية وتطور وتصقل بالدورات والندوات المتخصصة بعد ذلك. ان التطور المعرفي يجب ان يصاحبه تعديل تشريعي متي ما دعت الحاجة الية، فالتطور التقني متسارع فمع اشراق كل يوم جديد تطالعنا الشركات التجارية بما هو متطور ومستحدث , هذا التطور استغله ضعفاء النفوس في تسهيل ارتكاب الجريمة فكان التطور التقني خدمة يسرت وسهلت على الجناة ارتكاب جرائمهم ؛ وعلى الجانب الاخر اضحت النصوص التشريعية بعيدة كل البعد عن مواكبة هذا التطور وهي حقيقة يجب الاقرار بها ، ذلك ان التعديلات التشريعية لم توازي التطور التقني او تفي بالإحاطة بأنماط السلوك الممارس عن طريق تقنية المعلومات وعلى الرغم من ذلك فالأمر يستوجب ان تكون هناك رؤي واضحة وجهود تسعي لردم الهوه الفاصلة بين القصور التشريعي والتطور التقني والادراك المعرفي وبشكل يمنع او يحد من استغلال الجناة للتكنلوجيا لتحقيق مآرب غير مشروعة. ومن خلال هذه الورقة حاونا جاهدين قدر الاستطاع بيان مدي خطورة جرائم تقنية المعلومات واستظهار النقص والقصور المعرفي والادراكي بالجرائم الالكترونية واهمية رقي هذا الفهم في سبيل الحد من انتشار رقعة الجريمة الاكترونية ؛ وختاماً يمكن ان نضع بعض من التوصيات والتي يمكن الاسترشاد بها:

١- التوصية بإقرار مساق علمي يدرس بالجامعات يعنى بالجريمة الاكترونية وادلة اثباتها.

٢- نشر الوعي المعرفي بين المواطنين وخاصة الشباب بمخاطر التعامل مع المواقع والبرامج الالكترونية .

٣- تفعيل دور المجتمع المدني والمؤسسي للقيام بدوره التوعوي والوقائي.

٤- تدريب اعضاء الضبطية القضائية واعضاء السلطة القضائية للتعامل مع الجرائم الإلكترونية من خلال تبني برامج مشابهة كتلك المقررة في الاتحاد الاوروبي.

٥- تبني اصدار مجلة فصلية تعني بالجريمة الالكترونية.

٦- مراجعة التشريعات والاتفاقيات الخاصة بالجريمة الالكترونية نحو قوانيين محدثة وتعاون دولي فعال.

٧- التوصية بتبني انشاء فرق ضبط شرطية خاصة ومحاكم متخصصة بالجرائم الالكترونية.

المراجع

[١] انظر: www.oecd.org :

[٢] انظر: المادة رقم (١) من نظام مكافحة جرائم المعلوماتية السعودي.

[٣] انظر: المادة رقم (١) من القانون رقم (١٤) لسنة ٢٠١٤ م في شأن مكافحة الجرائم الالكترونية القطري.

[٤] مرسوم بقانون اتحادي رقم ٥ لسنة ٢٠١٢ م في شأن مكافحة جرائم تقنية المعلومات جاء استبدالا للقانون رقم (٦) لسنة ٢٠٠٦ م.

[٥] أنظر: د. محمد الشوا ، الغش المعلوماتي كظاهرة إجرامية مستحدثة ، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة ، ٢٨/٢٥ أكتوبر ١٩٩٣، ص ٢.

[٦] انظر: تقرير "The Norton Cybercrime Report 2013" ، http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

[٧] د. فايز بن عبدالله الشهري، التحديات الأمنية لوسائل الاتصال الجديدة – دراسة الظاهرة الإجرامية على شبكة الإنترنت، – دراسة الظاهرة الإجرامية على شبكة الإنترنت، المجلة العربية للدراسات الأمنية والتدريب، المجلد ٢٠، العدد ٣٩، (ص١٥٤ – وما بعدها).

[٨] هذة الدراسة شملت شريحة بلغت (٢٠٠) متخصص قانوني موزعين علي امارات الدولة السبع، استخدم فيها الباحث المنهج العلمي في جمع وتحليل البيانات.

[٩] اطلق على البرنامج مسمي (Cybex) شمل (٢١) دولة اوروبية و(٣) دول من امريكا الجنوبية.

[١٠] تعد هذة الدراسة من اهم الدراسات الميدانية ، استخدم فيها المنهج العلمي في جمع وتحليل البيانات ، حيث تم مقابلة اكثر من (١٢٥) شخص متخصص في مجالة من قضاة واعضاء نيابة وضباط شرطة ومحامين واكاديمين.